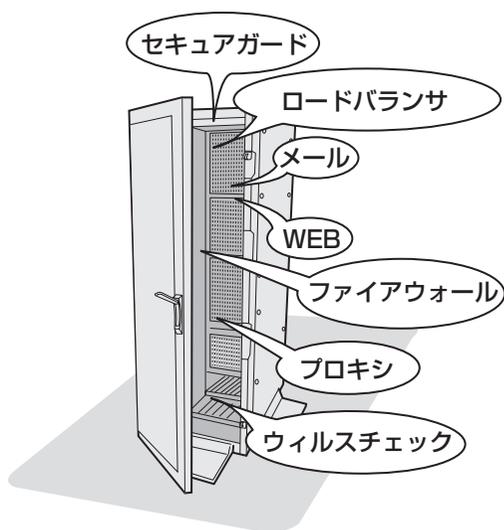
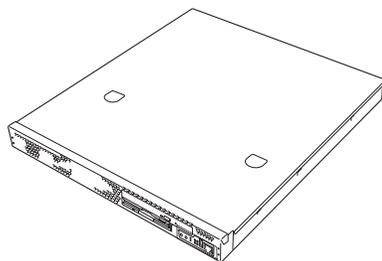
1 InterSecシリーズについて

本製品や添付のソフトウェアの特長、導入の際に知っておいていただきたい事柄について説明します。

InterSecシリーズとは

「オール・イン・ワン」から「ビルドアップ」へ。
お客様の運用目的に特化した設計で、必要のないサービス/機能を省き、セキュリティホールの可能性を低減し、インターネットおよびイントラネットの構築時に不可欠なセキュリティについて考慮して設計されてインターネットセキュリティ製品です。

1台のラックにそれぞれの機能を持つ装置を搭載(クラスタ構成可能)

InterSecシリーズの主な特長と利点は次のとおりです。

- **省スペース**

  設置スペースを最小限に抑えたコンパクトな筐体を採用。

- **運用性**

  運用を容易にする管理ツール。

- **クイックスタート**

  Webベースの専用設定ツールを標準装備。短時間(約5分)で初期設定を完了します。

- **高い信頼性**

  単体ユニットに閉じた動作環境で単機能を動作させるために、障害発生の影響は個々のユニットに抑えられます。また、絞り込まれた機能のみが動作するため、万一の障害発生時の原因の絞り込みが容易です。

- **高い拡張性**

  専用機として、機能ごとに単体ユニットで動作させているために用途に応じた機能拡張が容易に可能です。また、複数ユニットでクラスタ構成にすることによりシステムを拡張していくことができます。

- **コストパフォーマンスの向上**

  運用目的への最適なチューニングが行えるため、単機能の動作において高い性能を確保できます。また、単機能動作に必要な環境のみ提供できるため、余剰スペックがなく低コスト化が実現されます。

- **管理の容易性**

  環境設定や運用時における管理情報など、単機能が動作するために必要な設定のみです。そのため、導入・運用管理が容易に行えます。

InterSecシリーズには、目的や用途に応じて次のモデルが用意されています。

- **VCシリーズ(ウィルスチェック)**

  インターネット経由で受け渡しされるファイル(電子メール添付のファイルやWeb/FTPでダウンロードしたファイル)から各種ウィルスを検出/除去し、オフィスへのウィルス侵入、外部へのウィルス流出を防ぐことを目的とした装置です。

- **MWシリーズ(メール/WEB)**

  WebやFTPのサービスやインターネットを利用した電子メールの送受信や制御などインターネットで必要となるサービスを提供する装置です。

- **FWシリーズ(ファイアウォール)**

  CheckPoint FireWall-1を搭載し、高度なアクセス制御が可能な、大中規模の企業ネットワーク向けのファイアウォール専用機です。

- **SGシリーズ(ファイアウォール)**

  インターネットと接続した中小規模の企業ネットワークを外部からの不正なアクセスから守るファイアウォール専用機です。

- **LBシリーズ(ロードバランサ)**

  複数台のWebサーバへのトラフィック(要求)を整理し、負荷分散によるレスポンスの向上を目的とした装置です。

- **CSシリーズ(プロキシ)**

  Webアクセス要求におけるプロキシでのヒット率の向上(フォワードプロキシ)、Webサーバの負荷軽減・コンテンツ保護(リバースプロキシ)を目的とした装置です。

特長と機能

本装置の特長や本装置が提供する機能について説明します。

本装置は、インターネットゲートウェイ上でウイルスを検出、駆除して、企業LANへのウイルスの侵入、インターネットへのウイルス流出を防止することを目的として設計されたウイルス対策・アプライアンス製品です。
企業ネットワークにおけるウイルス対策およびコンテンツセキュリティ対策に必要な機能をオールインワンソリューションにて提供するトレンドマイクロ社のInterScan VirusWall for Small and Medium Businesses(以下、InterScan VirusWall)を、ウイルス対策エンジンとして採用しました。
また、本製品は必要なソフトウェアがすべてプリインストールされているため、短期間で導入／運用が可能です。本製品はInterScan VirusWallの全機能がプリインストールされています。
InterScan VirusWallは、SMTP、HTTP、FTP、POP3の4種類のトラフィックを監視可能です。

InterScan VirusWallでは、様々なネットワークトポロジや設定をサポートしています。4種類のプロトコルにおいて、柔軟なユーザ設定オプションが提供されており、ウイルス検出時の通知、ウイルスパターンの更新などの日常的なタスクを、自動的に実行するように予約することができます。
また、システム管理者は、ウイルス検索の対象となるファイルの種類、ウイルス検出時の処理(駆除、削除、隔離、放置)、その他の詳細な動作を設定することができます。
InterScan VirusWallでは、トレンドマイクロ社の32ビットマルチスレッド検索エンジンとパターンマッチングの手法を用いてウイルスを検出します。またInterScan VirusWallでは、既知のウイルスを検出するだけでなく、ポリモフィック型、ミューテーション型のウイルスも検出し、ネットワークへの感染を防止します。
さらに進んだウイルス対策を提供するために、InterScan VirusWallではトレンドマイクロ社のマクロウイルス検索エンジンMacroTrapを採用し、既知のマクロウイルスとその変種、亜種の両方を検出、駆除します。

InterScan VirusWallの仕組み

InterScan VirusWallでは、企業ネットワークとインターネット間のSMTP、HTTP、FTP、POP3トラフィックを監視します。InterScan VirusWallは検索対象のファイルを一時的な場所にコピーし、ウイルス検索を実行します。
ファイルがウイルスに感染していなければ、コピーを削除して、オリジナルのファイルを宛先に配信します。ウイルスを検出した場合は、設定に従って、次のような処理を実行します。

- ウイルスを駆除せずに、感染ファイルを「放置」します。感染ファイルは、任意の通知メッセージを添付して配信されます。
- ウイルスを駆除せずに、感染ファイルを「隔離」します。ファイルは配信されません。
- 感染ファイルを「削除」します。ファイルは配信されません。
- 感染ファイルのウイルスを「駆除」し、通常通り配信されるよう、元のサーバにファイルを送信します。駆除できなかった場合の二次処理として「隔離」または「削除」を選択できます。

● **通知**

InterScan VirusWallでは、ウイルス検出時、次の方法で通知を実行します。

- SMTP/POP3：オリジナルのメッセージに警告メッセージを挿入します。
- HTTP：要求元のブラウザにHTML形式の通知を送信します。
- FTP：要求元のクライアントにテキストの警告メッセージを送信します。

通知は自動的に実行され、SMTPの場合には、システム管理者、発信者、指定されている受信者に対して通知を実行できます。ウイルスが検出されなかった場合に、ウイルスに感染していなかったことを伝えるメッセージをE-Mailに添付することもできます。

重要

InterScan VirusWallの初期設定時に管理者の通知先を必ず設定してください。設定方法は、InterScanコンソールから[管理]→[設定]通知タブ画面の[通知先：]に管理者のe-mailアドレス、[SMTPサーバ:]、[ポート：]に送信先メールサーバのIPアドレスとポート番号を入力してください。

- **InterScan VirusWallでウイルスを検出する仕組み**

InterScan VirusWallは、「パターンマッチング」という手法を用いてウイルスを検出します。パターンマッチングでは、ウイルスパターンファイルに格納されている既知のウイルスシグネチャ(ウイルス識別コード)によってウイルスを識別します。検索対象のファイルからウイルスコード特有の文字列を抽出し、ウイルスシグネチャと比較して検出します。

ポリモフィック型／ミューテーション型ウイルスに関しては、InterScan VirusWallの検索エンジンで、検索対象のファイルを、一時的な環境内で実行します。ファイルが実行されると、ファイル内に暗号化されているウイルス識別コードが復号化されます。InterScan VirusWallでは、新たに復号化されたコードを含むファイル全体を検索して、ミューテーションウイルスのコード文字列を識別し、駆除、削除、移動(隔離)、放置など、あらかじめ指定した処理を実行します。

ウイルスパターンファイルを最新に保つことが大変重要です。ある統計によると、1年間に発生するウイルスの数は10000件以上におよび、毎日数種類のウイルスが誕生している計算になります。トレンドマイクロ社では、自動的な更新をサポートして、簡単にウイルスパターンファイルを更新できるようにしています。

MacroTrap

マクロウイルスは、短期間で蔓延するタイプのウイルスの1つです。マクロウイルスには、特定のオペレーティングシステムに限定されないという特徴があります。マクロウイルスはアプリケーションに依存するため、DOS、Windows、Macintosh、さらにはOS/2の垣根を越えて蔓延します。また、インターネットの普及によりウイルスがE-Mailによって一瞬にして世界中に広まることも考えられます。さらにマクロコードの機能の向上もあいまって、マクロウイルスは比較的感染力の強いウイルスといわれています。このようなマクロウイルスに対抗するためにトレンドマイクロ社では、高性能なMacroTrap技術を開発いたしました。MacroTrapにより、より確実にネットワークを保護できるようになります。

- **MacroTrapの仕組み**

MacroTrapでは、文書に関連するすべてのマクロコードに対して、ルールベース方式の検索を実行します。通常マクロウイルスのコードは、表に見えないテンプレート(たとえば、Microsoft Wordであれば、「.DOT」ファイル)の一部に組み込まれて、文書と一緒に移動します。トレンドマイクロ社のMacroTrapではこのテンプレートをチェックして、たとえば、テンプレートを部分的に他のテンプレートにコピーする命令(複製)や、危険なコマンドを実行する命令(破壊)など、ウイルスに類似した動作を実行する命令を探すことで、まだ知られていない亜種のマクロウイルスをチェックします。

- **圧縮ファイル**

VirusWallでは、圧縮ファイルを解凍し、各VirusWallのScan Filesオプションで指定されている検索条件に従って、その内容をチェックします。

VirusWallでは、最大20階層まで圧縮されているファイルを再帰的に検索します。つまりVirusWallでは、アーカイブにPK-ZIP、LZEXE、PK-LITE、Microsoft Compressを使って圧縮された「.cab」ファイルが入っている場合、圧縮ファイルが存在しなくなるか(その時点では、すべての圧縮ファイル内のファイルが検索されています)、上限値の20階層に達するまで、個々の階層を解凍します。

● MIMEエンコーディング

19種類の圧縮タイプ、最大20階層まで圧縮されているファイルのサポートに加えて、E-Mail検索では、UUencoding、Base64、quated-printable、BinHexでエンコードされたファイルをデコードすることができます。

InterScan VirusWallのユーザー登録

InterScan VirusWallのユーザー登録は大変重要です。
ユーザ登録することによって、InterScan VirusWallを使用するためのアクティベーションコードが提供されると共に、次のサービスを受けることができます。

－ 1年間のウイルスパターンファイル、検索エンジンの更新

－ 1年間のサポートサービス

－ 製品の最新情報の提供

上記サービスは弊社およびトレンドマイクロ社により提供されます。トレンドマイクロ社へのユーザー登録を行い、アクティベーションコードを取得してください。

本製品は、ウイルス検索、フィルタリング、ブロックなどの機能や、アップデート機能を利用する為にアクティベーションを実施する必要があります。アクティベーションの実施は、InterScanコンソールより[管理]→[製品ライセンス情報]を選択しアクティベーションコードを入力して[アクティベート]を実行します。ユーザ登録する際には、トレンドマイクロ社へのユーザ登録だけでなく、必ずWeb登録または、本製品に添付のFAX登録用紙によるFAX送付を使用してVirusCheckServerソフトウェアサポートサービスの登録およびサポート申し込みを行う必要があります。

お客様のユーザ登録(アクティベーションコード取得)の為のレジストレーションキーは、基本ライセンス製品パッケージに同梱しておりますので、ご使用ください。
本装置へもレジストレーションキーが同梱されております。InterScan VirusWallエンタープライズエディション(以下、InterScan VirusWall EE)ライセンスを既にお持ちで、そのライセンスにて本製品をご使用になる場合にご使用ください。
InterScan VirusWall EE ライセンスをお持ちの場合はVirusCheckServerソフトウェアサポートサービスの登録時にIMSS/IWSSのシリアル/アクティベーションコードの記載が必要です。

添付のディスクについて

本装置にはセットアップや保守・管理の際に使用するCD-ROMやフロッピーディスクが添付されています。ここでは、これらのディスクに格納されているソフトウェアやディスクの用途について説明します。

重要 添付のフロッピーディスクやCD-ROMは、システムのセットアップが完了した後でも、システムの再セットアップやシステムの保守・管理の際に使用する場合があります。なくさないように大切に保管しておいてください。

● バックアップCD-ROM

システムのバックアップとなるCD-ROMです。

再セットアップの際は、このCD-ROMと添付の「バックアップ CD-ROM用インストールディスク」を使用してインストールします。詳細は3章を参照してください。

「バックアップCD-ROM」には、システムのセットアップに必要なソフトウェアや各種モジュールの他にシステムの管理・監視をするための専用のアプリケーション「ESMPRO/ServerAgent」と「エクスプレス通報サービス」が格納されています。システムに備わったRAS機能を十分に発揮させるためにぜひお使いください。ESMPRO/ServerAgentの詳細な説明は「バックアップCD-ROM」内のオンラインドキュメントをご覧ください。エクスプレス通報サービスを使用するには別途契約が必要です。お買い求めの販売店または保守サービス会社にお問い合わせください。

● EXPRESSBUILDER(SE) CD-ROM

本体およびシステムの保守・管理の際に使用するCD-ROMです。

このCD-ROMには次のようなソフトウェアが格納されています。

− EXPRESSBUILDER(SE)

再セットアップの際に装置の維持・管理を行うためのユーティリティを格納するためのパーティション(保守パーティション)を作成したり、システム診断やオフライン保守ユーティリティなどの保守ツールを起動したりするときに使用します。詳細は5章を参照してください。

− DianaScope

システムが立ち上がらないようなときに、リモート(LAN接続またはRS-232Cケーブルによるダイレクト接続)で管理PCから本装置を管理する時に使用するソフトウェアです。詳細は5章を参照してください。

− ESMPRO/ServerManager

ESMPRO/ServerAgentがインストールされたコンピュータを管理します。詳細はEXPRESSBUILDER(SE)CD-ROM内のオンラインドキュメントを参照してください。

● 初期導入設定用ディスク(フロッピーディスク)

初期導入時の設定情報を書き込みます。設定情報の作成や変更をする「初期導入設定ツール」も含まれています。

● バックアップCD-ROM用インストールディスク(フロッピーディスク)

システムの再インストールの際に使用します。